Robust image watermarking based on two level DCT

Madhuri S. Hakke[1], Santosh S. Chowhan[2], Vikas T. Humbe[3]

[1]School of Technology, SRTMUN Sub-Centre, Latur, (M.S.), India.
[2]Associate Professor Symbiosis Institute of Computer Studies and research, Symbiosis International (Deemed University) Pune, (M.S.), India.
[3] Director, School of Technology, SRTMUN Sub-Centre, Latur, (M.S.), India.

Abstract- This paper presents a robust image watermarking scheme on gray level images, which is based on two level DCT (Discrete Cosine Transform) transform. In that first we compute the DCT of host image, then using the DC coefficients construct a low-resolution approximation image. Again we apply the DCT on the low-resolution approximation image and then added a pseudo-random noise sequence into its high frequencies. For watermark detection; from the watermarked image we extract the approximation image and then same noise sequence is generated. Experimental result shows that the hidden watermark is robust against many common attacks such as additive Gaussian noise, Salt and pepper noise addition, speckle noise addition and median filtering.

Keywords— *Blind digital watermarking, DCT, PSNR, NC.*

I. INTRODUCTION

Digital format of data is becoming more famous with advance research in information technology and computer network. But, digital data providers and owners encounter many problems from unauthorized copying and distribution. Digital watermark technology is proving very helpful to get protection against such unauthorized copying and distribution. We can apply watermark on text, image, audio and video.

Since centuries an identity card is stamped by steel seal to avoid forgery, painting is signed by the artists to test the copyright. Paper currency being identified by the embossed portrait. These methods can be traced back to many millionaires. They proved very helpful to identify the creator of art, picture, sculpture or document [1]. Information hiding can divide into three processes namely cryptography, steganography and watermark. Cryptography is a process in which intelligible data is converted into unintelligible data, the process which makes data difficult to be understood by unauthorized users. Decryption of cipher text can be done with the help of key by authorized users. Steganography hides information using a process which makes sense of information very difficult to be detected by attacker [2].

Electronic stamps, also conventionally called watermarks which are embedded into the images are one of solution for claiming the ownership possess following features -

- Undetectable by statistics;
- Difficult to detect for hackers;
- Impervious to image manipulation and processing operation likes filtering, cut-copy-past;
- Impervious to lossy data compression e.g., JPEG compression;
- Perceptually unable to be seen that is watermark is not expected to provide visible artifact [1].

Watermarking scheme can be classified as visible and invisible watermark. Another classification of watermarking is robust and fragile watermark [3]. Telediagnosis to telesurgery enhances the potential of medical information handling and sharing is possible because of advents of multimedia combined with information and communication technology.

In context of embedding domain, watermarking algorithms are classified into two groups [4] - spatial domain method which embeds the data by directly modifying the pixel values of original image and transform domain method which embed the data by modulating the transform domain coefficients. A frequency domain watermarking value of certain frequencies is altered from their original and embeds the watermark into the transformed image. This is more robust than the spatial domain technique. In frequency domain technique multiple transforms used for watermarking purpose such as DCT, DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform).

II. RELATED WORKS

They proposed [1] DCT based approach and embedding techniques can survive the cropping of an image, image enhancement and JPEG lossy compression. They used the multiple watermark and also multiresolution image structures with some modification about the choice of middle frequency coefficient.

In [5, 6, 7] survey of different techniques based on spatial domain (LSB) and the transform domain (DCT, DWT, DFT) presented. They had also presented a review of the significant techniques in existence for watermarking. They also presented aspects of watermarking and its application. For color image robust and secure watermarking algorithm in DCT-DWT is proposed [8].

Which frequency band in frequency domain can be robust and imperceptible to various attacks? According to Weber's rule, low frequency area is more robust than the middle and high frequency areas [9]. Therefore we propose the watermarking scheme based on low frequencies of DCT transform. Another watermarking algorithm based on DCT, DWT and SVD (Singular Value Decomposition) [10] and SVD is factorization of real or complex matrix. They described a watermark casting and detection scheme based on the SVD.

MATLAB simulation carried out for watermarking using both DCT and DWT algorithm; that shows the simulation time for DCT is 1.48 sec and 0.9 for DWT for same image. Therefore conclusion is DWT is much faster than DCT [11]. They had presented [12] method for embedding and detecting a chaotic watermark in large images based on segmenting the image and locating regions that are robust to several image manipulations. In order to derive a robust region representation of the original image an adaptive clustering technique is employed. The robust regions are approximated by ellipsoids, whose bounding rectangles are chosen as the embedding area for the watermark. The watermark is geometrically adapted before embedding using the orientation, centre coordinates and dimensions of the bounding rectangle.

In [9] they also use two levels DCT based algorithm of watermarking with wavelet packet denoising and spread spectrum communication techniques. Most of the energy of natural images is concentrated in the lower frequency range. Therefore, information hidden in the higher frequency components are quantizes and discards by lossy compression method. However noise in lower frequency components than the higher frequency is more sensitive for human eye. Invisibly embed the watermark that can survive lossy data compressions, so the trade-off is to embed the watermark as low energy pseudo-random noise sequences into the low-frequency range of the image [9].

In [13] proposed new scheme for color image watermarking based on color quantization technique. In this watermark embedding process is put on pixel mapping process of color quantization process. When pixel mapping process is performed at the same time watermark is embedded. And at the same time of image decoding procedure watermark extraction is executed. Some techniques are proposed in which the watermark is embedded in the middle and high frequency component. These techniques are vulnerable to attacks such as compression and noise addition. In our paper we assume Kerckhoffs' principle in that opponent knows the all aspects of the authentication system except the secret key that is shared between transmitter and receiver.

Also watermarking is done on text and combined image and text. In that first watermark is embedded into text then watermark key is generated, after that encrypt the text with RSA algorithm [14]. In [15] proposed new algorithm based on combined DLT and DWT. In that watermark is embedded in special middle frequency coefficient sets of three levels DWT transformed of a host image followed by computing 4×4 block based DLT on the selected DWT coefficient sets.

III. PROPOSED METHOD

In our paper, we propose watermarking scheme which is based on DCT transform. In this method we apply the DCT on original image. Each bit of watermark is scattered in 64 blocks of the original image. Because of embedding the watermark in low frequency we obtain the robustness and get the imperceptibility by scattering the watermarks bit in different block.

To judge the robustness we calculate the PSNR (Peak Signal-to-Noise Ratio) and NC (Normalized Cross-Correlation). For watermarked images PSNR values are all greater than 38 dB, which is empirical value for the image without any perceivable degradation [9].

A. Embedding Algorithm

In this paper, our host image is of size 512×512. We apply DCT on 8×8 non overlapping blocks of host image. After that low resolution approximation image (LRAI) is generated by selecting DC coefficient out of the 64 DCT coefficients for each 8×8 transformed block of host image. Therefore the size of extracted LRAI is always 1/64 of the host image. If the size of host image is 512×512 then the size of extracted LRAI is 64×64 pixels.

Again extracted LRAI is divided into 8×8 non overlapping blocks and apply the DCT on it. Then according to the value of watermark bit a pseudo random noise sequence is added to the high frequencies of DCT transform of LRAI using following eq. [9].

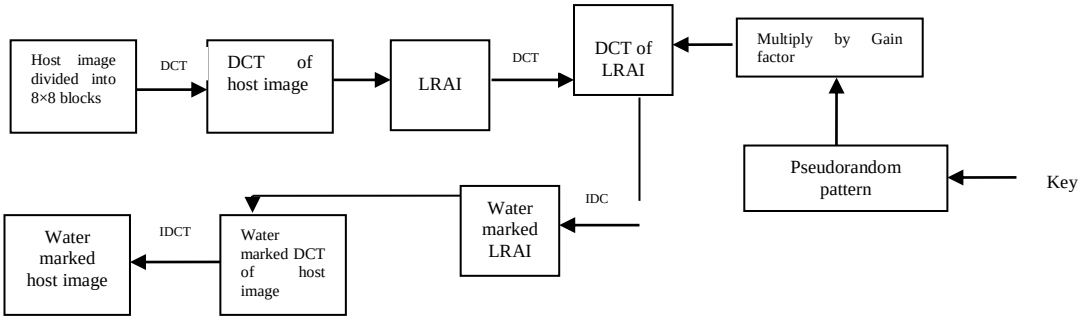

Fig. 1: Watermark embedding process

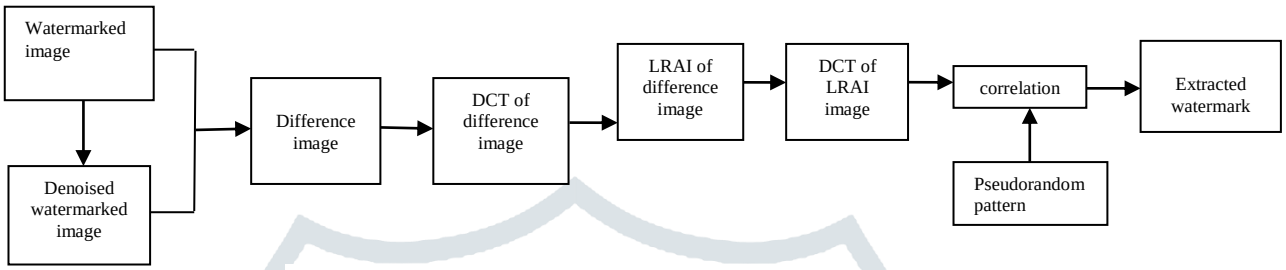

Fig. 2: Watermark extraction process

$$L^{w}_{x,y}(u,v) = \begin{cases} L_{x,y}(u,v) + k \times W^{i}_{x,y}(u,v), & u,v \in F_H \\ \mathrm{L}_{x,y}(u,v), & u,v \notin F_H \end{cases} \quad (1)$$

In eq. (1) L denotes DCT transform of LRAI, F_H is the high frequency band, k the gain factor, (u,v) the DCT coefficient in the corresponding 8×8 block of L, (x,y) is the location of an 8×8 block of LRAI and W^i the pseudo random noise sequence according to the value of i.

We are used two separate pseudo random noise sequences to present the bit value of 0 and 1. Then take inverse transformed of each block to give watermarked LRAI. Finally host image is watermarked and then compute the IDCT of watermarked LRAI. We have used two different pseudo random noise sequences that are as-

key1 =[0 1 -1;1 0 -1;1 -1 0;-1 1 0; 1 1 0;-1 -1 0; 0 0 1;0 0 -1]
Key2 =[1 -1 -1;-1 0 1;1 0 -1;1 0 0;-1 0 0;0 -1 1;-1 0 -1;0 1 1]

Since only one bit of watermark is in each block of LRAI. So for size of host image 512×512, watermark size is limited to 8×8 pixels. That is the size of host image is $2^n \times 2^n$, so the size of extracted LRAI will be $2^{n-3} \times 2^{n-3}$ and size of watermark will be $2^{n-6} \times 2^{n-6}$. Fig. (1) shows the watermark embedding process.

B. *Extracted algorithm*

In extraction algorithm same pseudo random pattern is use to detect the watermark. If we use the different key then different sequence of random no. is generated. Therefore watermark will not detect by the extraction algorithm. When we add the watermark at that time noise is also added to the host image. So in extraction algorithm first denoise the image. Denoised image is subtracted from the watermarked image then we get the new image. That new image indicates the noise added to the host image during embedding watermark. Fig. (2) shows the watermark extraction process.

Follow the same steps from the embedding algorithm; from the difference image transformed LRAI is constructed. Correlation between transformed LRAI with both noise patterns is computed. If the higher correlation is obtained with noise pattern 1, then a watermark bit of 1 is detected. Similar way for watermark bit 0. Finally, the hidden watermark in difference image is extracted by the given algorithm. Fig. (4) shows the difference image between watermarked image and denoised image.

IV. EXPERIMENTAL RESULT AND DISCUSSIONS

We have implemented our method on different standard images of size 512×512. In fig. (3), 8×8 watermark pattern is shown which is embedded in the host image. On cameraman test image which is watermarked with gain factor 35 and extracted watermark is shown in fig. (5). We use another 5 different standard gray scale images (Lena, livingroom, pirate, woman_blonde, woman_darkhair)

In our proposed method, we calculate the PSNR and NC. Whereas the PSNR to calculate the difference between the original image and watermarked image or attacked watermarked image [9]. PSNR is calculated by eq. (2)

$$PSNR = 10\log_{10}\frac{M_1 \times M_2 \times \max(f(i,j))^2}{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[f(i,j) - f'(i,j)]^2}(dB) \quad (2)$$

Where $M_1 \& M_2$ are the size of image, $f(i,j)$ is the original image, $f'(i,j)$ is the watermarked image or attacked watermarked image.

Also we compute the NC to analyze the similarity of the original watermark and extracted watermark [9].

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j) \times W'(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W(i,j)]^2} \times \sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W'(i,j)]^2}} \quad (3)$$

Where $M_1 \& M_2$ the size of watermark image, $W(i,j)$ is the original watermark and $W'(i,j)$ is the extracted watermark. Fig. (2) shows the watermark extraction process. Several common signal processing attacks were also applied to the watermarked image such as Gaussian noise addition, salt and pepper noise addition, speckle noise addition and median filtering. The trade-off between visual quality and watermark robustness is about gain factor 25 to 35. So in our proposed method we used gain factor 35.

1. Additive Gaussian white noise –
   White Gaussian noise with 0.05 variance is added to the watermarked image to test the robustness of the method. 19.1460 dB is the PSNR value after adding Gaussian noise. Fig. (6) Shows the watermarked image after Gaussian noise addition.

2. Salt and pepper noise –
   Salt and pepper noise with intensity value of 0.4 to the watermarked image. The intensity value specifies the percentage of image pixel values that are affected by the noise. Watermarked image attacked by salt and pepper noise which drops its PSNR to 9.04 dB. Fig. (7) Shows the watermarked image after salt and pepper noise addition.
   .

3. Multiplicative speckle noise –
   Watermark image is attacked by another multiplicative speckle noise with variance is 0.1; in this speckle noise add to the watermarked image in a multiplicative war rather than an additive way. PSNR value by speckle noise is 15.7722 dB. Fig. (8) Shows the watermarked image after multiplicative speckle noise addition.

4. Median filter –
   Median filter is usually used to reduce noise. We use median filter (5×5) to reduce noise of watermarked image and PSNR value is 30.7773 dB. Fig. (9) Shows the watermarked image after median filter.

Fig. 3. Original image and watermark

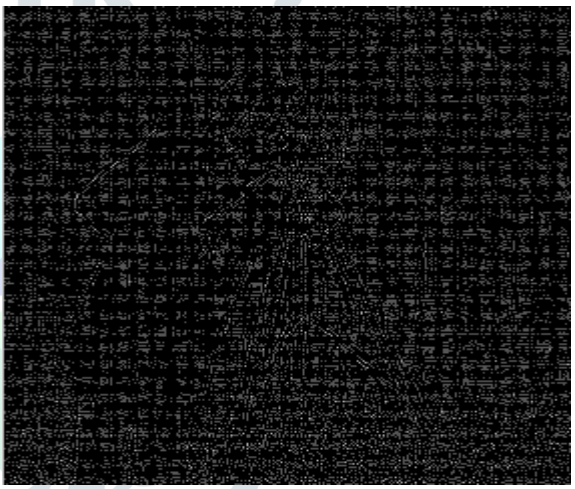

Fig. 4: Difference image between watermarked image and denoised image

Fig. 5: Watermarked image and extracted watermark

Fig. 6: Watermarked image under Gaussian noise attack (variance=0.05)

Fig. 7: Watermarked image under salt and pepper noise attack (intensity= 0.4)

Fig. 8: Watermarked image under multiplicative speckle noise attack (variance=0.1

Fig. 9: Watermarked image after being median filter (5×5)

V. CONCLUSION

In this paper, we proposed a two level DCT based blind digital watermark. We embed the watermark in low frequency therefore; we get the robust watermark against many attacks such as additive Gaussian noise, salt and pepper noise addition, speckle noise addition. In experimental work we calculate the NC and PSNR to judge the robustness and invisibility of watermark.

In our future work, we will try the algorithm for the color image and more than one watermark will be embedded in image.

REFERENCES

[1] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden digital watermark in images," *IEEE Trans on Image Processing*, vol. 8, no. 1, pp. 58-68, Jan 1999.

[2] Dr. Ajit, Preeti Kalra and Sonia Dhull, "Digital watermarking," ISSN: 2277-128X, *International Journal of Advanced Research in Computer Science and Software Engineering*," vol. 3, Issue 4, pp. 280-283, April 2013.

[3] Chin-Shiuh Shieh, Hsiang-Cheh Huang, Feng-Hsing Wang and Jeng-Shyang Pan, "Genetic watermarking based on transform domain techniques, *Elsevier, Pattern Recognition* 37, pp. 555-565, 2004.

[4] Radhika V. Totla and K. S. Bapat, "Comparative analysis of watermarking in digital images using DCT and DWT," ISSN: 2250-3153, *International Journal of Scientific and Research Publications*, vol. 3, Issue 2, pp. 1-4, Feb. 2013.

[5] Namita Tiwari and Sharmila, "Digital watermarking applications parameter measures and techniques," *International Journal of Computer Science and Network Security*, vol. 17, no. 3, pp. 184-194, March 2017.

[6] Lalit Kumar Saini and Vishal Shrivastava, "A survey of digital watermarking technique and its application," ISSN: 2347-8578, *International Journal of Computer Science Trends and Technology*, vol. 2, Issue 3, pp. May-June 2014.

[7] Kunal D. Megha, Nimesh P. Vaidya and Asst. Prof. Ketan Patel, "Digital watermarking: Data hiding techniques using DCT-DWT algorithm," ISSN: 2319-5940, *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, Issue 6, pp. 2397-2402 , June 2013.

[8] Md. Saiful Islam and Ui Pil Chong, "A digital image watermarking algorithm based on DCT DWT and SVD," *International Journal of Computer and Communication Engineering*, vol. 3, no. 5, pp. 356-360, Sep. 2014.

[9] A. H. Taherinia and M. Jamzad, "A robust image watermarking using two level DCT and wavelet packets denoising," *International Conference in Availability, Reliability and Security*, pp. 150-157, 2009.

[10] Arisudan Tiwari, Anoopa Arya and Shubham Shukla, "Digital watermarking analysis using DCT and DWT," ISSN: 2394-6598, *International Journal of Emerging Technology and Innovative Engineering*, vol. 1, Issue 6, pp. 11-23, June 2015.

[11] Athanasios Nikolaidis and Ioannis Pitas, "Region-based image watermarking," *IEEE trans on Image Processing*, vol. 10, no. 11, pp. 1726-1740, Nov. 2001.

[12] Piyu Tsai, Yu-Chen Hu and Chin-Chen Chang, "A color image watermarking scheme based on color quantization," *Elsevier, Signal Processing* 84, pp. 95-106, 2004.

[13] Jaseena K. U. and Anita John, "Text watermarking using combined image and text for authentication and protection," *International Journal of Computer Application* (0975-8887), vol. 20, no. 4, pp. 8-13, April 2011.

[14] Yusuf Perwej, Firoj Parwej and Asif Perwej, "Copyright protection of digital images using robust watermarking based on joint DLT and DWT," ISSN: 2229-5518, *International Journal of Scientific and Engineering Research*, vol. 3, Issue 6, pp. 1-9, Junen2012.

[15] Frank Y. Shih and Scott Y. T. Wu, "Combinational image watermarking in the spatial and frequency domains," *Elsevier, Pattern Recognition* 36, pp. 969-975, 2003.

[16] Wei Lu, Hongtao Lu and Fu-Lai Chung, "Feature based watermarking using watermark template match," *Elsevier, Applied Mathematics and Computation* 177, pp. 377-386, 2006.

[17] Vengadapathiraj M., Rajendhiran V., Gururaj M., Shatishkumar R. and Anbarasu M., "Comparison of different digital watermarking technique for content authentication," *International Journal of Science, Engineering and Technology research*, vol. 3, Issue 11, pp. 3031-3038, Nov. 2014.

[18] Chetna, "Digital image watermarking using DCT," ISSN: 2320-088X, *International Journal of Computer Science and Mobile Computing*, vol. 3, Issue 9, pp. 586-591, Sep. 2014.

[19] Manpreet Kaur and Sheenam Malhotra, "Review paper on digital image watermarking technique for robustness," ISSN: 2277-128X, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, Issue 5, pp. 948-952, May 2014.

[20] Huiping Guo, Nicolas D and Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme," *Springer, Multimedia System*, pp. 1-11, 2003.

[21] Smita Pandey and Rohit Gupta, "A comparative analysis on digital watermarking with techniques and attacks," ISSN: 2277-128X, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, Issue 6, pp. 101-107, June 2016.

[22] Shraddha S. Katariya (Patni), "Digital watermarking: Review," ISSN: 2277-3754, *International Journal of Engineering and Innovative Technology*, vol. 1, Issue 2, pp. 143-153, Feb. 2012.